Logiciel

smb.conf : le fichier de configuration de Samba

Le fichier **/etc/samba/smb.conf** est le seul fichier de configuration de Samba. Ce fichier est composé de sections (dont le nom est entre crochets) :

[global]
: paramètres généraux et les paramètres par défaut des différents partages

[printers] et [print$]
: spécifiques au partage d'imprimantes,

[homes]
: Partage du répertoire personnel d'un utilisateur (son répertoire $HOME)
Il apparaîtra dans la liste des partages avec le nom d'utilisateur du client (s'il est identifié),

[le_nom_d'un_partage]
: Pour chaque partage

Les **commentaires** débutent par un point-virgule (**;**) ou un dièse (**#**). Toutes lignes commençant par un de ces symboles ne seront pas interprétées par Samba.

[global] = paramètres généraux

workgroup
: groupe de travail dans lequel votre serveur apparaîtra lorsqu'il sera interrogé par les clients.
Note that this parameter also controls the Domain name used with the security = domain setting.
Par défaut: **workgroup = WORKGROUP**
Exemple : workgroup = MYGROUP

log file
: Nom du fichier journal Samba (également appelé fichier de débogage).
Pas de valeur par défaut
Exemple : log file = /usr/local/samba/var/log.%m

un fichier journal par machine plutôt qu'un fichier global.
Facilite la lecture des journaux.

max log size
: taille maximale du fichier journal en kilo-octets
Si la taille est dépassée, Samba renomme le fichier en ajoutant une extension .old
Une taille de 0 signifie aucune limite.
Par défaut: **max log size = 5000**
Exemple : max log size = 1000

logging

Ce paramètre configure les backends de journalisation
Plusieurs backends peuvent être spécifiés en même temps, avec différents niveaux de journalisation pour chaque backend.
Le paramètre est une liste de backends, où chaque backend est spécifié comme backend[:option][@loglevel].
Le paramètre 'option' peut être utilisé pour transmettre des options spécifiques au backend.
Le niveau de journalisation d'un backend est facultatif, s'il n'est pas défini pour un backend, tous les messages sont envoyés à ce backend.
Le niveau de journalisation des paramètres détermine les niveaux de journalisation globaux, tandis que les niveaux de journalisation spécifiés ici définissent ce qui est envoyé aux différents backends.
Lorsque la journalisation est définie, elle remplace les paramètres syslog et syslog uniquement.
Certains backends ne sont disponibles que lorsque Samba a été compilé avec les bibliothèques supplémentaires.
Liste des backends de journalisation :

- syslog
- file
- systemd
- lttng
- gpfs
- ringbuf :

Le backend ringbuf prend un argument facultatif **ringbuf:size=NBYTES** pour modifier la taille de la mémoire tampon utilisée, la valeur par défaut est de 1 Mo

Par défaut: **logging =**
Exemple: logging = syslog@1 file

panic action

option de développement qui permet d'appeler une commande système lorsque smbd plante.
Généralement utilisé pour attirer l'attention sur un problème qui est survenu.
Par défaut: **panic action =**
Exemple: panic action = “/bin/sleep 90000”

server role

Mode de fonctionnement du serveur Samba
Par défaut: **server role = auto** → Samba fonctionne selon le paramètre de sécurité ou s'il n'est pas spécifié comme un simple serveur de fichiers qui n'est connecté à aucun domaine.
Les alternatives sont server role = standalone ou server role = member server, qui relie Samba à un domaine Windows, ainsi que server role = domain controller, qui exécute Samba en tant que contrôleur de domaine Windows.
Utilisez server role = standalone et map to guest pour configurer des partages sans mot de passe (partages invités).
SERVER ROLE = AUTO

Valeur par défaut de server role, oblige Samba à consulter le paramètre

security (s'il est défini) pour déterminer server role

SERVER ROLE = STANDALONE

Si security n'est pas non plus spécifié, c'est le paramètre de sécurité par défaut dans Samba.
En fonctionnement autonome, un client doit d'abord se connecter avec un nom d'utilisateur et un mot de passe valides (qui peuvent être mappés à l'aide du paramètre de mappage de nom d'utilisateur) stockés sur cette machine.
Les mots de passe chiffrés (voir le paramètre encrypted passwords) sont utilisés par défaut dans ce mode de sécurité.
Les paramètres tels que user et guest only s'ils sont définis sont ensuite appliqués et peuvent modifier l'utilisateur UNIX à utiliser sur cette connexion, mais uniquement après l'authentification de l'utilisateur.

SERVER ROLE = MEMBER SERVER

Ce mode ne fonctionnera correctement que si net a été utilisé pour ajouter cette machine dans un domaine Windows.
Suppose que le paramètre encrypted passwords soit défini sur yes.
Dans ce mode, Samba essaiera de valider le nom d'utilisateur / mot de passe en le passant à un contrôleur de domaine Windows ou Samba, comme le ferait un serveur Windows.
Notez qu'un utilisateur UNIX valide doit toujours exister ainsi que le compte sur le contrôleur de domaine pour permettre à Samba d'avoir un compte UNIX valide auquel mapper l'accès aux fichiers. Winbind peut fournir cela.

SERVER ROLE = CLASSIC PRIMARY DOMAIN CONTROLLER

Ce mode de fonctionnement exécute un contrôleur de domaine principal Samba classique, fournissant des services de connexion de domaine aux clients Windows et Samba d'un domaine de type NT4.
Les clients doivent être joints au domaine pour créer un chemin sécurisé et approuvé sur le réseau.
Il ne doit y avoir qu'un seul PDC par étendue NetBIOS (généralement un réseau de diffusion ou des clients desservis par un seul serveur WINS).

SERVER ROLE = CLASSIC BACKUP DOMAIN CONTROLLER

Ce mode de fonctionnement exécute un contrôleur de domaine de sauvegarde Samba classique, fournissant des services de connexion de domaine aux clients Windows et Samba d'un domaine de type NT4.
En tant que contrôleur secondaire de domaine, cela permet à plusieurs serveurs Samba de fournir des services de connexion redondants à une seule étendue NetBIOS.

SERVER ROLE = ACTIVE DIRECTORY DOMAIN CONTROLLER

Ce mode de fonctionnement exécute Samba en tant que contrôleur de domaine Active Directory, fournissant des services de connexion de domaine aux clients Windows et Samba du domaine. Ce rôle nécessite une configuration spéciale.

Par défaut: **server role = AUTO**

Exemple: server role = ACTIVE DIRECTORY DOMAIN CONTROLLER

obey pam restrictions

Lorsque Samba 3.0 est configuré pour activer la prise en charge de PAM (c'est-à-dire –with-pam), ce paramètre contrôlera si Samba doit ou non obéir aux directives de gestion de compte et de session de PAM.

Le comportement par défaut consiste à utiliser PAM uniquement pour l'authentification en texte clair et à ignorer tout compte ou gestion de session.

Notez que Samba ignore toujours PAM pour l'authentification dans le cas encrypt passwords = yes.

Par défaut : **obey pam restrictions = no**

unix password sync

Ce paramètre booléen contrôle si Samba tente de synchroniser le mot de passe UNIX avec le mot de passe SMB lorsque le mot de passe SMB chiffré dans le fichier smbpasswd est modifié.

Si cette option est définie sur yes, le programme spécifié dans le paramètre de programme passwd s'appelle AS ROOT - pour permettre au nouveau mot de passe UNIX d'être défini sans accéder à l'ancien mot de passe UNIX (car le code de changement de mot de passe SMB n'a pas accès à l'ancien mot de passe en clair, seulement au nouveau).

Cette option n'a aucun effet si samba s'exécute en tant que active directory domain controller.

Par défaut : **unix password sync = no**

passwd program

Nom d'un programme qui peut être utilisé pour définir les mots de passe utilisateur UNIX. Toutes les occurrences de %u seront remplacées par le nom d'utilisateur.

L'existence du nom d'utilisateur est vérifiée avant d'appeler le programme de changement de mot de passe.

Notez également que de nombreux programmes passwd insistent sur des mots de passe raisonnables, tels qu'une longueur minimale, ou l'inclusion de caractères et de chiffres à casse mixte.

Cela peut poser un problème car certains clients (tels que Windows pour Workgroups) mettent le mot de passe en majuscule avant de l'envoyer.

Notez que si le paramètre unix password sync est défini sur yes, ce programme est appelé comme ROOT avant que le mot de passe SMB du fichier smbpasswd ne soit modifié.

Si cette modification du mot de passe UNIX échoue, smbd ne pourra pas non plus modifier le mot de passe SMB (c'est par conception).

Si le paramètre de synchronisation de mot de passe unix est défini, ce paramètre DOIT UTILISER DES CHEMINS ABSOLUS pour TOUS les programmes appelés et doit être examiné pour les implications de sécurité.

Notez que par défaut, unix password sync est définie sur non.

Par défaut : **passwd program =**

Exemple: passwd program = /bin/passwd %u

passwd chat

Cette chaîne contrôle le dialogue qui a lieu entre smbd et le programme de changement de mot de passe local pour changer le mot de passe de l'utilisateur.

La chaîne décrit une séquence de questions-réponses que smbd utilise pour déterminer ce qu'il faut envoyer au programme passwd et à quoi s'attendre.

Si la sortie attendue n'est pas reçue, le mot de passe n'est pas modifié.

Cette séquence de discussion est souvent assez spécifique au site, en fonction des méthodes locales utilisées pour le contrôle des mots de passe (comme NIS, etc.).
Notez que ce paramètre n'est utilisé que si le paramètre unix password sync est défini sur yes.
Cette séquence est alors appelée comme ROOT lorsque le mot de passe SMB dans le fichier smbpasswd est modifié, sans accès à l'ancien texte en clair du mot de passe.
Cela signifie que root doit pouvoir réinitialiser le mot de passe de l'utilisateur sans connaître le texte du mot de passe précédent.
La chaîne peut contenir la macro %n pour le nouveau mot de passe.
L'ancien mot de passe (%o) n'est disponible que si encrypt passwords a été désactivé.
La séquence de discussion peut également contenir les macros standard \n, \r, \t et \s pour donner un saut de ligne, un retour chariot, une tabulation et un espace.
La chaîne de séquence de discussion peut également contenir un * qui correspond à n'importe quelle séquence de caractères.
Les guillemets doubles peuvent être utilisés pour rassembler des chaînes contenant des espaces en une seule chaîne.
Si la chaîne d'envoi dans n'importe quelle partie de la séquence de discussion est un point ".", aucune chaîne n'est envoyée.
De même, si la chaîne attendue est un point, aucune chaîne n'est attendue.
Si le paramètre de changement de mot de passe pam est défini sur yes, les paires de conversation peuvent être mises en correspondance dans n'importe quel ordre, et le succès est déterminé par le résultat PAM, et non par une sortie particulière.

La macro \n est ignorée pour les conversions PAM.

Par défaut : **passwd chat = *new*password* %n\n *new*password* %n\n *changed***
Exemple passwd chat = "*Enter NEW password*" %n\n "*Reenter NEW password*" %n\n "*Password changed*"

pam password change

S'il est activé, PAM sera utilisé pour les changements de mot de passe à la demande d'un client SMB au lieu du programme répertorié dans le programme passwd.
Il devrait être possible de l'activer sans changer votre paramètre de discussion passwd pour la plupart des configurations.
Par défaut : **pam password change = no**

map to guest

Ce paramètre peut prendre quatre valeurs différentes, qui indiquent à smbd quoi faire avec les demandes de connexion utilisateur qui ne correspondent pas à un utilisateur UNIX valide d'une manière ou d'une autre.
Les quatre paramètres sont:

Never

Signifie que les demandes de connexion utilisateur avec un mot de passe invalide sont rejetées. C'est la valeur par défaut.

Bad User

Signifie que les connexions utilisateur avec un mot de passe non valide sont rejetées, sauf si le nom d'utilisateur n'existe pas, auquel cas il est traité comme une connexion invité et mappé dans le compte guest.

Bad Password

Signifie que les connexions utilisateur avec un mot de passe non valide sont traitées comme une connexion guest et mappées dans le compte guest.

Notez que cela peut causer des problèmes car tout utilisateur qui ne saisit pas correctement son mot de passe sera silencieusement connecté en tant que “invité” - et ne saura pas la raison pour laquelle il ne peut pas accéder aux fichiers qu'il pense devoir - aucun message ne lui aura été envoyé qu'ils se sont trompés de mot de passe.

Bad Uid

S'applique uniquement lorsque Samba est configuré dans un certain type de sécurité en mode domaine (security = {domain|ads}) et signifie que les connexions utilisateur qui sont authentifiées avec succès mais qui n'ont pas de compte utilisateur Unix valide (et que smbd est incapable d'en créer un) devraient être mappés au compte invité défini.
Notez que ce paramètre est nécessaire pour configurer les services de partage “Invité”.
En effet, dans ces modes, le nom de la ressource demandée n'est pas envoyé au serveur tant que le serveur n'a pas authentifié le client avec succès, de sorte que le serveur ne peut pas prendre de décisions d'authentification au bon moment (connexion au partage) pour les partages “Invité”.

Par défaut : **map to guest = Never**
Exemple: map to guest = Bad User

usershare allow guests

Ce paramètre contrôle si les partages définis par l'utilisateur sont accessibles ou non aux utilisateurs non authentifiés.
Cela équivaut à permettre aux personnes qui peuvent créer un partage de définir guest ok = yes dans une définition de partage.
En raison de sa nature sensible à la sécurité, la valeur par défaut est désactivée.
Par défaut : **usershare allow guests = no**

guest ok = yes/no

(synonyme : public)

server string = nomduserveur

identification de la machine (habituellement quelque chose comme *Serveur Samba*)

hosts allow = adresses IP

variable très importante pour la sécurité du réseau : définit les adresses IP autorisées à contacter le serveur Samba. Exemple : **192.168.0. 192.168.5. 127.** autorise les machines ayant une adresse IP du réseau local **192.168.0.xxx** et **192.168.5.xxx**. **127.** permet d'autoriser les connexions sur l'adresse loopback à des fins de test.

printcap name = /etc/printcap

load printers = yes

Ces deux variables permettent de charger automatiquement les imprimantes du système au lieu de les configurer individuellement.

printing = système

système de gestion d'impression à utiliser. Les choix possibles sont **bsd**, **sysv**, **plp**, **lprng**, **aix**, **hpux** ou **qnx**.

guest account = login

nom d'un utilisateur invité. Il est impératif de l'ajouter au système. Sinon, l'utilisateur **nobody** est utilisé par défaut.

security = type

gestion de la sécurité :

- par utilisateur (user)
- ou par serveur (server).

password server = nomdeserveur
: avec la gestion de sécurité par le serveur : précise un nom de serveur.

password level =
user level =
: taille minimum pour le mot de passe et le nom d'utilisateur.

encrypt passwords = yes
: Active le cryptage du mot de passe. Ne pas oublier le **s** dans le nom de variable, souvent source d'erreurs.

smb passwd file = /etc/smbpasswd
: fichier de mots de passe cryptés.

unix password sync = yes
passwd program = /usr/bin/passwd %u
passwd chat = * New * UNIX * password * %n\n * ReType * new * UNIX * password * %n\n * passwd: * all * authentification * tokens * updated * successfully *
: Ces variables autorisent une synchronisation des mots de passe SMB avec ceux de la machine Unix
Attention, c'est inutile si on veut seulement autoriser le changement de mot de passe SMB. Un mauvais choix ici peut s'avérer catastrophique pour la politique de sécurisation.

username map = fichier
: spécifie un fichier d'utilisateurs différents de celui du système.

include = /chemin/smb.conf %m
: intègre des paramètres supplémentaires en fonction du nom NetBIOS du demandeur. %m représente le nom NetBIOS.

socket options = TCP_NODELAY
: Améliore souvent les performances réseau. D'autres astuces dans le fichier speed.txt livré avec la documentation de Samba

interfaces = adresses IP
: adresses IP des interfaces réseau en cas d'utilisation de plusieurs périphériques.

local master = no
: exclut le serveur Samba pour qu'il ne devienne pas un serveur membre (voir LMF 4)

os level = chiffre
: niveau de compétence du serveur dans l'élection sur serveur primaire. inutile si local master = no.

domain master = yes
: le serveur Samba peut être serveur de domaine et collecter des informations pour tenir à jour sa propre table de sous-réseau. A ne pas activer si le réseau possède déjà une machine NT qui fait ce travail.

preferred master = yes
: Déclenche une élection de serveurs primaires au démarrage → augmente les chances du serveur Samba d'être élu.

domain controller = nomdeserveur
: nom d'une machine NT qui joue le rôle de serveur de domaine primaire.

name resolve order = wins lmhosts bcast
: ordre dans lequel se fera la résolution des noms et des adresses IP. Ce paramètre vise à optimiser la vitesse du système.

wins support = yes
: Active la résolution WINS (Windows Internet Name Serving)

dns proxy = yes

Demande à Samba d'utiliser la fonction nslookups pour la résolution des noms NetBIOS.

preserve case = no

Désactive ou active la préservation de la casse des caractères.

default case = lower

casse par défaut : minuscule (à l'opposé de upper pour majuscule)

case sensitive = no

Désactive la gestion de la casse des caractères.

[homes]

comment

champ de texte qui s'affiche à côté d'un partage lorsqu'un client interroge le serveur, soit via le voisinage du réseau, soit via net view pour répertorier les partages disponibles.
Par défaut : **comment = # No comment**
Exemple: comment = Fred's Files

browseable

Ceci contrôle si ce partage est vu dans la liste des partages disponibles dans une vue réseau et dans la liste de navigation.
Par défaut : **browseable = yes**

read only

Un synonyme inversé est writeable.
Si ce paramètre est yes, les utilisateurs d'un service ne peuvent pas créer ou modifier des fichiers dans le répertoire du service.
Notez qu'un service imprimable (printable = yes) autorisera TOUJOURS l'écriture dans le répertoire (si les privilèges de l'utilisateur le permettent), mais uniquement via des opérations de spoule.
Par défaut : **read only = yes**

create mask

Lors de la création d'un fichier, les autorisations nécessaires sont calculées en fonction du mappage des modes DOS aux autorisations UNIX, et le mode UNIX résultant est alors «ET» bit par bit avec ce paramètre.
Ce paramètre peut être considéré comme un MASQUE bit par bit pour les modes UNIX d'un fichier.
Tout bit non défini ici sera supprimé des modes définis sur un fichier lors de sa création.
La valeur par défaut de ce paramètre supprime le groupe et les autres bits d'écriture et d'exécution des modes UNIX.
Suite à cela, Samba fait un “OU” bit à bit du mode UNIX créé à partir de ce paramètre avec la valeur du paramètre de mode de création forcée qui est 000 par défaut.
Ce paramètre n'affecte pas directory masks.
Par défaut : **create mask = 0744**
Exemple: create mask = 0775

directory mask

Ce paramètre correspond aux modes octaux utilisés lors de la conversion des modes DOS en modes UNIX lors de la création de répertoires UNIX.
Lors de la création d'un répertoire, les autorisations nécessaires sont calculées en fonction du mappage des modes DOS aux autorisations UNIX, et une opération “ET” bit à bit entre le mode UNIX résultant et ce paramètre.
Ce paramètre peut être considéré comme un MASQUE bit par bit pour les modes UNIX d'un répertoire.

Tout bit non défini ici sera supprimé des modes définis sur un répertoire lors de sa création.
La valeur par défaut de ce paramètre supprime les bits d'écriture «groupe» et «autres» du mode UNIX, ce qui permet uniquement à l'utilisateur propriétaire du répertoire de le modifier.
Après cela, Samba effectuera un 'OU' bit par bit sur le mode UNIX créé à partir de ce paramètre avec la valeur du paramètre force directory mode.
Ce paramètre est défini à 000 par défaut (c'est-à-dire qu'aucun bit de mode supplémentaire n'est ajouté).
Par défaut : **directory mask = 0755**
Exemple: directory mask = 0775

valid users
liste d'utilisateurs autorisés à se connecter à ce service.
Les noms commençant par «@», «+» et «&» sont interprétés selon les mêmes règles que celles décrites dans le paramètre utilisateurs non valides.
Si ce champ est vide (par défaut), n'importe quel utilisateur peut se connecter.
Si un nom d'utilisateur figure à la fois dans cette liste et dans la liste des utilisateurs non valides, l'accès est refusé pour cet utilisateur.
%S est remplacé par servicename actuel. Utile dans la section [homes].
Remarque: Lorsqu'il est utilisé dans la section [global], ce paramètre peut avoir des effets secondaires indésirables.
Par exemple: Si samba est configuré comme MASTER BROWSER, cette option empêchera les postes de travail de naviguer sur le réseau.
Par défaut : **valid users =** # No valid users list (anyone can login)
Exemple: valid users = greg, @pcusers

comment = Home Directories
commentaire ou très court descriptif.
browseable = no
Interdit le parcours du répertoire.
défaut : **yes**
writable = yes
Synonyme inversé pour **read only**.
Par défaut : writeable = no (ou read only = yes)
Autorise l'écriture dans le répertoire.

Autres :

guest ok = yes/no
(synonyme : public)
force user = yes/no
(synonyme : public)

Autres sections

Les autres sections déterminent les ressources susceptibles d'être partagées.

Exemple 1

Une ressource disque appelée toto sera déclarée comme suit :

```
[toto]
comment = essai de partage
path = /home/samba/toto
public = yes
writable = yes
printable = no
write list = @totogrp
```

- Emplacement physique sur la machine Unix : /home/samba/toto.
- Répertoire public non imprimable (ce n'est pas une ressource d'impression).
- Peut être parcouru et lu par tous les utilisateurs,
- Permission d'écriture limitée au groupe totogrp.

Exemple 2

Dans le cas d'une imprimante [priprime] la section sera

```
[priprime]
comment = Imprimante de test
valid users = nicolas
path = /home/nicolas
printer = nicolas_printer
public = no
writable = no
printable = yes
```

Ici, la ressource est imprimable, mais non inscriptible. Cette ressource est réservée à l'utilisateur nicolas et n'est donc pas public. Dernier point, le chemin de la ressource est placé dans le répertoire personnel de l'utilisateur d'où l'intérêt de pouvoir y écrire sans pour autant avoir la permission de le parcourir.

Conclusion

Notre parcours du fichier smb.conf est à présent terminé.

Nous venons de voir les options les plus importantes, mais il en existe bien d'autres. Pour toutes les connaître, tapez man smb.conf. Vous pouvez également lire l'importante documentation fournie avec Samba et habituellement placée dans /usr/doc.

Voir aussi

- **(fr)** Le fichier de configuration de Samba : smb.conf
- **(fr)** http://okki666.free.fr/docmaster/articles/linux028.htm

---

Basé sur « Samba : le fichier de configuration » par Linux Magazine France Avril 99.